4

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/616,680	07/09/2003	John Apostolopoulos	200209975-1	2579

22879 7590 01/31/2007

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	**PAPER NUMBER**
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/616,680	APOSTOLOPOULOS ET AL.	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 July 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail.Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 30-44 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 30 comprises two portions, a truncatable unit and a cryptographic checksum. Considering a data structure to be "a physical or logical relationship among data elements, designed to support specific data manipulation functions" (IEEE Standard Dictionary of Electrical and Electronic Terms 308, 5th edition, 1993), this is considered non-functional descriptive material that does not constitute a statutory process, machine, manufacture, or composition of matter.

Claim Objections

3. Claim 8 is objected to because of the following informalities: examiner believes that claim 8 should be dependent on claim 2, instead of claim 1, because of the introduced "media data" in claim 2. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claim 43 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Claim 43 recites the limitation "said transcoder readable header." There is insufficient antecedent basis for this limitation in the claim.

Double Patenting

7. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

8. Claims 1-44 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-34 of copending Application No. 10/698,784. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant application separates data into segments, computes checksums for the data segments, and ***combines the segments together into a packet***; whereas the copending application

partitions data into segments, calculates a checksum for the data segments, and ***enables transmitting of a first checksum separately from the rest of the data packet***. The bold, italicized parts above show the differences between the instant application and copending application. The difference between the two applications is that the data segments that have checksums are operated on (transmitted, encrypted, decrypted, etc.) separately from the rest of the data segments (see, for example, claim 10 of the instant application).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1-5, 7, 8, 11-14, 16, 17, 19-22, 30, 36, 37, and 44 are rejected under 35 U.S.C. 102(a/e) as being anticipated by Meehan et al. (U.S. Patent Pub. No. 2003/0103571).

Regarding claim 1, Meehan et al. teaches a method of ensuring integrity of data, comprising:

- Separating an amount of data into segments (fig. 1, ref. num 3 and 4);
- Computing a cryptographic checksum for a said segment (paragraph 0042); and
- Combining a segment and an associated cryptographic checksum into a data packet (fig. 1, ref. num 7).

Regarding claim 2, Meehan et al. teaches wherein said data comprises media data (paragraph 0039).

Regarding claim 3, Meehan et al. teaches wherein said data comprises secure scalably streamable data (fig. 1, ref. num 3 and 4).

Regarding claim 4, Meehan et al. teaches wherein said data is transmittable in a network (fig. 1, ref. num 7).

Regarding claim 5, Meehan et al. teaches wherein said data is stored in a storage medium (paragraph 0004).

Regarding claim 7, Meehan et al. teaches further comprising forwarding said data packet (fig. 1, ref. num 7).

Regarding claim 8, Meehan et al. teaches wherein said media data to be streamed comprises a plurality of said data packets (fig. 1, ref. num 3 and 4).

Regarding claim 11, Meehan et al. teaches wherein said cryptographic checksum is computed for a truncatable unit in said segment (paragraph 0003).

Regarding claim 12, Meehan et al. teaches wherein said segment comprises a plurality of said truncatable units (paragraph 0004).

Regarding claims 13 and 19, Meehan et al. teaches wherein a cryptographic checksum is computed for each of said truncatable units in said segment (paragraph 0042).

Regarding claims 14 and 20, Meehan et al. teaches wherein a first cryptographic checksum is calculated for a first truncatable unit, and wherein a second cryptographic checksum is calculated for the combination of a second truncatable unit, said first truncatable unit, and said first cryptographic checksum (paragraph 0006-0010, suggests scalability is provided across multiple computing devices with varying processing abilities, thus allowing portions of the data to be "truncated" to provide lower quality to devices with lower processing power and providing more "truncated" portions for devices with higher processing power).

Regarding claim 16, Meehan et al. teaches a method for providing security to a scalably streamed media signal in a network, comprising:

- Separating said streaming media signal into a plurality of truncatable units (fig. 1, ref. num 3 and 4);
- Computing a cryptographic checksum for each of said truncatable unit (paragraph 0042);
- Appending said associated cryptographic checksum onto each of said truncatable units (fig. 1, ref. num 5);
- Combining one or more of said truncatable units and associated cryptographic checksums into a transmittable data packet (fig. 1, ref. num 6); and
- Forwarding said data packet (fig. 1, ref. num 7).

Regarding claim 21, Meehan et al. teaches wherein the size of said truncatable units is selected to ensure the size of said data packet is transmittable in said network (page 4, table 1).

Regarding claim 22, Meehan et al. teaches wherein said associated cryptographic checksum is computed independently for its associated truncatable unit (paragraph 0042).

Regarding claim 30, Meehan et al. teaches a computer readable medium having a data packet stored therein for causing a functional change in the operation of a device, said data packet comprising:

- A plurality of truncatable units, each of said units comprising an amount of media data (fig. 1, ref. num 3 and 4); and
- A cryptographic checksum computed for each of said truncatable units (fig. 1, ref. num 5 and paragraph 0042).

Regarding claim 36, Meehan et al. teaches wherein said cryptographic checksum is computed based on one truncatable unit (paragraph 0042).

Regarding claim 37, Meehan et al. teaches wherein said cryptographic checksum is computed based on a plurality of truncatable units and associated checksums (paragraph 0042).

Regarding claim 44, Meehan et al. teaches wherein each of said truncatable units is enabled to be deleted from said transmittable packet independently of other truncatable units in said packet (paragraph 0006-0010, suggests scalability is provided across multiple computing devices with varying processing abilities, thus allowing portions of the data to be "truncated" to provide lower quality to devices with lower processing power and providing more "truncated" portions for devices with higher processing power).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 6, 9, 10, 15, 17, 18, 23-29, 31-35, and 38-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meehan et al. (U.S. Patent Pub. No. 2003/0103571) in view of Chang et al. (U.S. Patent No. 6,963,972).

Regarding claims 6 and 17, Meehan et al. teaches all the limitations of claim 1, above. However, Meehan et al. does not teach further comprising applying a transcoder-readable header to said data packet.

Chang et al. teaches further comprising applying a transcoder-readable header to said data packet (col. 10, lines 54-62).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine further comprising applying a transcoder-readable header to said data packet, as taught by Chang et al., with the method of Meehan et al. It would have been obvious for such modifications because the transcoder readable header enables transcoding, which allows changes in quality without having to decrypt the data.

Regarding claims 9 and 23, Meehan et al. teaches all the limitations of claim 1, above. However, Meehan et al. does not teach further comprising encrypting said segment and said cryptographic checksum.

Chang et al. teaches further comprising encrypting said segment and said cryptographic checksum (col. 4, lines 5-9).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine encrypting the data, as taught by Chang et al., with the method of Meehan et al. It would have been obvious for such modifications because encryption secures sensitive data from unauthorized viewers.

Regarding claims 10, 18, and 27, Meehan et al. as modified by Chang et al. teaches wherein said packet is enabled to be decrypted independently of other packets comprising said streamed media data (see paragraph 0042 of Meehan et al. and fig. 12 of Chang et al.).

Regarding claims 15, 24, and 38, Meehan et al. teaches all the limitations of claim 1, above. However, Meehan et al. does not teach wherein said cryptographic checksum is computed using a hash function.

Chang et al. teaches wherein said cryptographic checksum is computed using a hash function (col. 12, lines 19-35).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using a hash, as taught by Chang et al., with the method of Meehan et al. It would have been obvious for such modifications because hashes provide tamper protection (see col. 12, lines 19-25 of Chang et al.).

Regarding claim 25, Meehan et al. teaches further comprising accessing said data packet (fig. 1, ref. num 2) and forwarding said data packet (fig. 1, ref. num 7).

Meehan et al. does not teach reading a transcoder-readable header of said data packet and deleting one or more of said truncatable units.

Chang et al. teaches reading a transcoder-readable header of said data packet (col. 10, lines 54-62) and deleting one or more of said truncatable units (col. 13, lines 28-43); and

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine deleting one or more of said truncatable units, as taught by Chang et al., with the method of Meehan et al. It would have been obvious for such modifications because the transcoder readable header enables transcoding, which

allows changes in quality without having to decrypt the data. Deleting units allows lower quality data to be transmitted to low-end devices.

Regarding claim 26, Meehan et al. as modified by Chang et al. teaches further comprising:

- Writing a new transcoder-readable header for said data packet reflecting said deleting and applying said new transcoder-readable header to said data packet (see col. 13, lines 36-43 of Chang et al.).

Regarding claim 28, Meehan et al. as modified by Chang et al. teaches wherein said deleting comprises transcoding said data packet (see col. 13, lines 28-43 of Chang et al.).

Regarding claim 29, Meehan et al. as modified by Chang et al. teaches wherein said transcoder-readable header comprises information related to the content of said data packet while leaving said truncatable units undecrypted (see col. 13, lines 28-43 of Chang et al.).

Regarding claim 31, Meehan et al. teaches all the limitations of claim 30, above. However, Meehan et al. does not teach wherein said data packet further comprises a transcoder readable header comprising information related to said truncatable units and said cryptographic checksums.

Chang et al. teaches wherein said data packet further comprises a transcoder readable header comprising information related to said truncatable units and said cryptographic checksums (col. 10, lines 54-62).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine wherein said data packet further comprises a transcoder readable header comprising information related to said truncatable units and said cryptographic checksums, as taught by Chang et al., with the medium of Meehan et al. It would have been obvious for such modifications because the transcoder readable header enables transcoding, which allows changes in quality without having to decrypt the data.

Regarding claim 32, Meehan et al. as modified by Chang et al. teaches wherein said transcoder readable header enables transcoding said data packet (see col. 13, lines 28-43 of Chang et al.).

Regarding claim 33, Meehan et al. as modified by Chang et al. teaches wherein said truncatable units and said cryptographic checksums are enabled to be encrypted independently of said transcoder readable header (see paragraph 0042 of Meehan et al. and fig. 12 of Chang et al.).

Regarding claim 34, Meehan et al. as modified by Chang et al. teaches wherein said truncatable units and said cryptographic checksums are enabled to be decrypted independently of said transcoder readable header (see paragraph 0042 of Meehan et al. and fig. 12 of Chang et al.).

Regarding claim 35, Meehan et al. as modified by Chang et al. teaches wherein said transcoder readable header is enabled to be read independently of said truncatable units and said cryptographic checksums (see paragraph 0042 of Meehan et al. and fig. 12 of Chang et al.).

Regarding claim 43, Meehan et al. as modified by Chang et al. teaches wherein said transcoder readable header is enabled to be written independently of said truncatable units and said cryptographic checksums (see paragraph 0042 of Meehan et al. and fig. 12 of Chang et al.).

Regarding claims 39-42, Meehan et al. teaches all the limitations of claim 30, above. However, Meehan et al. does not teach wherein said cryptographic checksum is calculated using a message digest, message authentication code, keyed-hashing-for-message-authentication, and a digital signature function.

Chang et al. does not teach wherein said cryptographic checksum is calculated using a message digest, message authentication code, keyed-hashing-for-message-authentication, and a digital signature function (col. 9, lines 32-37).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine calculating the checksum using a variety of different functions, as taught by Chang et al., with the medium of Meehan et al. It would have been obvious for such modifications because hashes provide tamper protection (see col. 12, lines 19-25 of Chang et al.).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Brandon Hoffman

BH

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/26/07